IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A data communication apparatus having a memory space, the data communication apparatus managing the memory space by separating the memory space into one or more file systems, the apparatus comprising:

authenticating means for requesting performance of ~~one of~~ a mutual authentication ~~and a verification for a security code~~ for each file system to be accessed from an external apparatus or a program, the mutual authentication including a key associated with a service provider of the external apparatus or the program designated at a time of creation of the file system wherein the key is not provided as an input from a user;

authentication information managing means for managing, for each file system, whether the file system is in an authentication-required state in which performance of ~~one of~~ the mutual authentication ~~and the verification for the security code~~ is requested or in a release state in which the access is permitted after ~~the one of~~ the mutual authentication ~~and the verification for the security code~~ is completed; and

state managing means for returning the file system from the release state to the authentication-required state in response to an occurrence of a predetermined event.

Claim 2 (Original): The data communication apparatus according to Claim 1, wherein, when one of the external apparatus and the program changes the accessing file system to another file system, the state managing means resets the release state of the original accessing file system to the authentication-required state.

Claim 3 (Currently Amended): The data communication apparatus according to Claim 1, wherein the state managing means resets the file system from the release state ~~of the original accessing file system~~ to the authentication-required state after a predetermined period

of time has elapsed since the file system was changed to the release state or after a predetermined period of time has elapsed since the data communication apparatus was powered on.

Claim 4 (Currently Amended): A method for managing a memory of a data communication apparatus, the data communication apparatus having a memory space and managing the memory space by separating the memory space into one or more file systems, the method comprising the steps of:

(a) requesting performance of ~~one of~~ a mutual authentication ~~and a verification for a security code~~ for each file system to be accessed from an external apparatus or a program, the mutual authentication including a key associated with a service provider of the external apparatus or program designated at a time of creation of the file system wherein the key is not provided as input from a user;

(b) managing, for each file system, whether the file system is in an authentication-required state in which performance of ~~one of~~ the mutual authentication ~~and the verification for the security code~~ is requested or in a release state in which the access is permitted after ~~one of~~ the mutual authentication ~~and the verification for the security code~~ is completed; and

(c) returning the file system from the release state to the authentication-required state in response to an occurrence of a predetermined event.

Claim 5 (Currently Amended): The method for managing a memory of a data communication apparatus according to Claim 4, wherein, when one of the external apparatus and the program changes the accessing file system to another file system, step (c) resets the file system from the release state ~~of the original accessing file system~~ to the authentication-required state.

Claim 6 (Currently Amended): The method for managing a memory of a data communication apparatus according to Claim 4, wherein step (c) resets the file system from the release state ~~of the original accessing file system~~ to the authentication-required state after a predetermined period of time has elapsed since the file system was changed to the release state or after a predetermined period of time has elapsed since the data communication apparatus was powered on.

Claim 7 (New): The data communication apparatus according to Claim 1, wherein the authenticating means verifies a security code.

Claim 8 (New): The data communication apparatus according to Claim 7, wherein the security code includes a Personal Identification Number (PIN).

Claim 9 (New): The data communication apparatus according to Claim 7, wherein the authentication information means further comprises determining whether the file system is in an authentication-required state in which performance of the verification of the security code is requested or in a release state in which the access is permitted after the verification of the security code is completed.

Claim 10 (New): The method for managing a memory of a data communication apparatus according to Claim 4, wherein step (a) further comprises requesting performance of a verification for a security code for each file system to be accessed from an external apparatus or a program.

Claim 11 (New): The method for managing a memory of a data communication apparatus according to Claim 10, wherein step (b) further comprises managing, for each file

system, whether the file system is in an authentication-required state in which performance of the verification of the security code is requested or in a release state in which the access is permitted after the verification for the security code.

Claim 12 (New): The method for managing a memory of a data communication apparatus according to Claim 10, wherein the security code includes a Personal Identification Number (PIN).

Claim 13 (New): A data communication apparatus having a memory space, the data communication apparatus managing the memory space by separating the memory space into one or more file systems, the apparatus comprising:

a first file system associated with a first key designated by a supplier of the data communication apparatus; and

a second file system associated with a second key designated by a service provider that has been granted permission by the supplier to use an area of the memory space identified by an area id,

wherein following a mutual authentication including the area id and the second key access to the second file system is granted.

Claim 14 (New): The data communication apparatus of Claim 13, wherein the first and second keys are encrypted.

Claim 15 (New): The data communication apparatus of Claim 13, wherein access to the second file system is provided by encrypted communications encrypted by the second key.

Claim 16 (New): The data communication apparatus of Claim 13, wherein the first file system further comprises a plurality of application areas and access to at least one of the application areas is allowed only after a verification of a security code.

Claim 17 (New): The data communication apparatus of Claim 13, wherein the second file system further comprises a plurality of application areas and access to at least one of the application areas is allowed only after a verification of a security code.